FortiAuthenticator™ 3.3
What's New Guide

FortiAuthenticator™ 3.3 What's New Guide

February 5, 2015

Revision 1

Technical Documentation	http://help.fortinet.com
Knowledge Base	http://kb.fortinet.com
Forums	https://support.fortinet.com/forums
Customer Service & Support	https://support.fortinet.com
Training	http://training.fortinet.com
FortiGuard Threat Research & Response	http://www.fortiguard.com
License Agreement	http://www.fortinet.com/doc/legal/EULA.pdf
Document Feedback	Email: techdocs@fortinet.com

Table of contents

Change Log

Revision	Date	Change Description
1	2015-02-05	Initial Release

Introduction

This document lists and describes many of the new features added to FortiAuthenticator™ 3.3. For a complete list of all new FortiAuthenticator™ 3.3 features and bug fixes, please see the latest release notes.

This document, and all of the FortiAuthenticator™ 3.3 documentation, will continue to improve as we see the new features in action and as we get feedback about these documents from you. You can send comments and suggestions for improvements for all FortiAuthenticator™ 3.3 documents to techdoc@fortinet.com.

What's New

FortiAuthenticator™ 3.3 is a feature release however only contains a minimal number of features which were not available in time for the 3.2 release. This release also introduces an important security fix for CVE-2015-0235, also known informally as GHOST, a vulnerability caused by a gethostbyname() heap overflow in the glibc library.

System features

These are features related to general system operation and not a specific functional area.

Load balancing HA

The load balancing high availability method has been designed to enable active-active high availability across geographically separated locations and layer 3 networks. This feature only supports synchronization of authentication related features including:

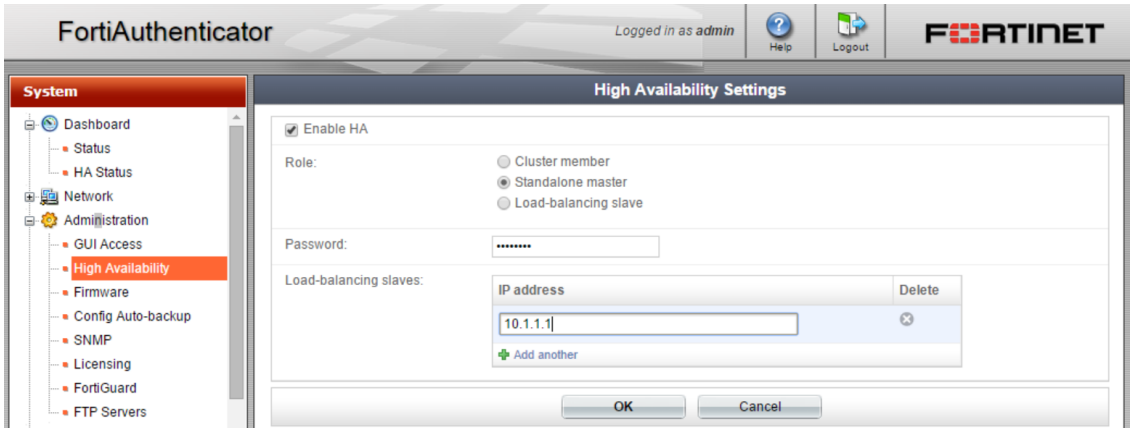
- Token and seeds
- Local User DB
- Remote User DB
- Group mappings
- Token/user mapping

Other features such as general configuration, FSSO, certificates etc are not synchronized between devices.

There are two new HA Roles:

Standalone Master – The primary system where users, groups and tokens are added/deleted.

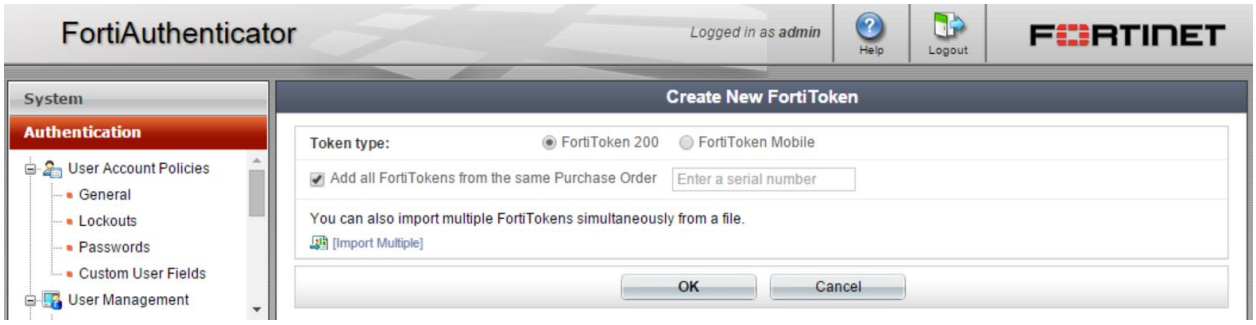
Load-balancing slave – Slave devices to which the primary authentication features are synchronized.



To enable resilience of the master system, it is possible to configure an Active-Passive Master cluster with load balanced slave devices. Up to 2 slave devices are supported.

Authentication

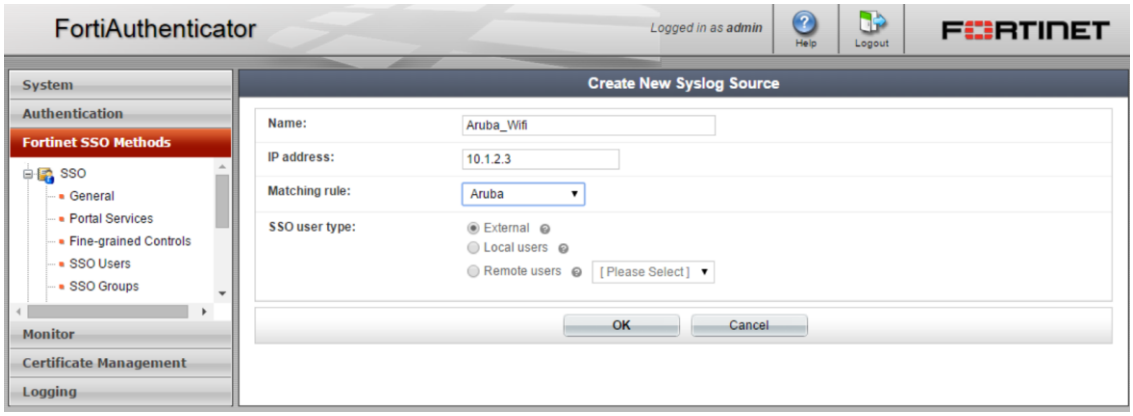
In order to simplify import of large numbers of tokens, a new option Add all FortiTokens from the same purchase order has been added. By enabling this feature and entering a single token; all tokens associated with that order will be imported.



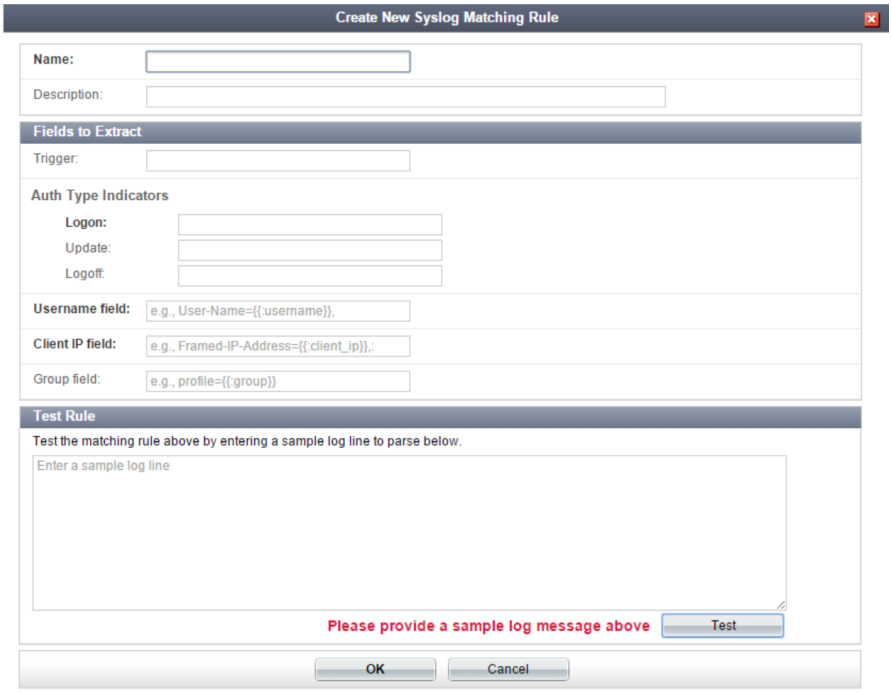
FSSO

Syslog to FSSO

FortiAuthenticator supports the ability to take in and parse username and IP address information from Syslog and use this to inject into FSSO for use in FortiGate or FortiCache Identity Based Policies. Predefined policies are available for Cisco and Aruba wireless controllers.



For other systems, custom based policies are supported to parse log files in various formats.


Create New Syslog Matching Rule
Name:
Description:
Fields to Extract
Trigger:
Auth Type Indicators
Logon:
Update:
Logoff:
Username field:
e.g., User-Name={{:username}},
Client IP field:
e.g., Framed-IP-Address={{:client_ip}},
Group field:
e.g., profile={{:group}}
Test Rule
Test the matching rule above by entering a sample log line to parse below.
Enter a sample log line
Please provide a sample log message above
Test
OK
Cancel